

WHAT IS CLAIMED IS:

- 1 1. Certification processing hardware connected to a terminal device capable of
2 communicating with a server device via a network and executing user certification processing of a
3 user of the terminal device by communicating with the server device, the certification processing
4 hardware comprising:
 - 5 a storing unit which stores certification information of the user;
 - 6 an encryption key receiving unit which requests a certification process from the server
7 device and receives an encryption key assigned to the certification process hardware from the
8 server device;
 - 9 an encryption processing unit which encrypts the certification information by using the
10 received encryption key;
 - 11 a certification information transmitting unit which transmits the encrypted certification
12 information to the server device;
 - 13 a certification result information receiving unit which receives encrypted certification result
14 information from the server device;
 - 15 a decryption processing unit which decrypts the encrypted certification result information
16 by using the encryption key; and
 - 17 an execution permitting unit which gives an execution permission for a process comprising
18 communication from the server device to the terminal device when a decryption of the certification
19 result information by the decryption processing unit succeeds.
- 1 2. The certification processing hardware according to claim 1, wherein the decryption

2 processing unit executes a decryption process by using one encryption key only once.

1 3. The certification processing hardware according to claim 1, further comprising a
2 controller which controls the terminal device based on the decrypted certification result
3 information.

1 4. A certification processing system comprising:

2 a server device and a terminal device which can communicate with each other via a
3 network, and hardware which is connected to the terminal device and executes a user certification
4 process in the terminal device by communicating with the server device, wherein the server device
5 comprises:

6 an encryption key transmitting unit which transmits an encryption key assigned to the
7 hardware which is making a certification request in response to the certification request from the
8 hardware; and

9 a certification result information transmitting unit which receives and decrypts encrypted
10 certification information from the hardware and encrypts certification result information to transmit
11 an encrypted certification result information to the hardware, and wherein the hardware comprises:

12 a storing unit which stores certification information of the user;

13 an encryption key receiving unit which sends the certification request to the server device
14 and receives the encryption key from the server device;

15 an encryption processing unit which encrypts the certification information by utilizing the
16 received encryption key;

17 a certification information transmitting unit which transmits the encrypted certification

18 information to the server device;

19 a certification result information receiving unit which receives the encrypted certification

20 result information from the server device;

21 a decryption processing unit which decrypts the encrypted certification result information

22 by using the encryption key; and

23 an execution permitting unit which gives execution permission of a process comprising

24 communication from the server device to the terminal device when decryption of the certification

25 result information by the decryption processing unit succeeds, and wherein the terminal device

26 comprises:

27 a permission requesting unit which requests the execution permission of the process

28 comprising the communication from the server device to the hardware; and

29 an executing unit which executes the process after receiving the execution permission from

30 the hardware.

1 5. Use management hardware which is connected to a terminal device and executes a

2 managing process of availability of the terminal device, the use management hardware comprising:

3 a storing unit which stores availability information indicating the availability of the terminal

4 device;

5 a receiving unit which receives an operation request from the terminal device;

6 a determining unit which determines the availability of the terminal device based on the

7 availability information; and

8 a controller which enables the terminal device to operate when the determining unit

9 determines that the terminal device is available.

1 6. A method for performing user certification processing for a user of a terminal device
2 communicating with a server device via a network, the method comprising the steps of:
3 connecting certification processing hardware to the terminal device;
4 storing certification information of the user in the certification processing hardware;
5 requesting a certification process from the server device;
6 receiving, from the server device, an encryption key assigned to the certification processing
7 hardware;
8 encrypting the certification information by using the received encryption key;
9 transmitting the encrypted certification information to the server device;
10 receiving encrypted certification result information from the server device;
11 decrypting the encrypted certification result information by using the encryption key; and
12 giving an execution permission of a process comprising communication from the server
13 device to the terminal device after the decrypting step.

1 7. The method according to claim 6, wherein the decrypting step is executed by using one
2 encryption key only once.

1 8. The method according to claim 6, further comprising the step of controlling the terminal
2 device based on the decrypted certification result information.

1 9. A method for performing user certification processing for a user of a terminal device
2 communicating with a server device via a network, the method comprising the steps of:
3 connecting certification processing hardware to the terminal device;

4 storing certification information of the user in the certification processing hardware;

5 sending a certification request from the certification processing hardware to the server

6 device;

7 transmitting from the server device an encryption key assigned to the certification

8 processing hardware in response to the certification request; and

9 encrypting the certification information by utilizing the received encryption key;

10 transmitting the encrypted certification information to the server device;

11 receiving encrypted certification information from the certification processing hardware;

12 decrypting the encrypted certification information;

13 encrypting certification result information;

14 transmitting the encrypted certification result information to the certification processing

15 hardware;

16 receiving the encrypted certification result information from the server device;

17 decrypting the encrypted certification result information by using the encryption key; and

18 giving execution permission of a process comprising communication from the server device

19 to the terminal device after the decrypting the encrypted certification result information step; and

20 executing the process after receiving the execution permission from the hardware.

1 10. A method for performing use management of a terminal device, the method

2 comprising the steps of:

3 storing availability information indicating the availability of the terminal device;

4 receiving an operation request from the terminal device;

5 determining the availability of the terminal device based on the availability information;

6 and

7 enabling the terminal device to operate when the determining step determines that the
8 terminal device is available.